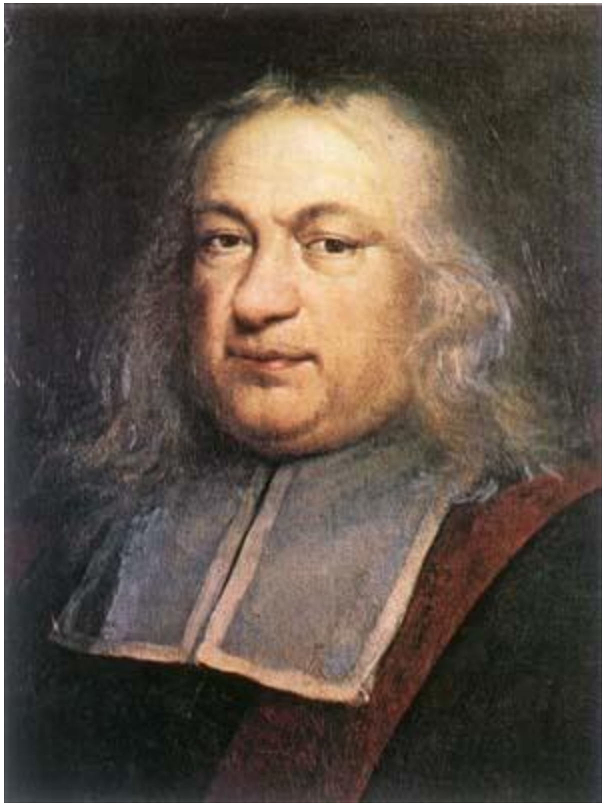
Today's Agenda

- Wrap up of Number Theory (Sec. 3.7)
  - Fermat's Little Theorem
  - Public Key Cryptography (RSA)
- Strings and Languages (Chap. 12)

Fermat's little theorem:

For any prime p and
integer a not divisible by p
$(\gcd(a, p) = 1)$:

$$a^{p-1} \equiv 1 \pmod{p}$$



Pierre de Fermat
(1601-1665)

Example: $a = 2$ $\qquad$ $p = 5$

$$2^4 = 16 \equiv 1 \pmod{5}$$

(We will use FLT in the RSA cryptosystem)

Public Key Cryptography (RSA cryptosystem)

"MEET YOU IN THE PARK"

encryption

$$f(x) = x^e \bmod n$$

decryption

$$f^{-1}(y) = y^d \bmod n$$

"938377290938363746 7"

$$n = p \cdot q$$

Large primes

n, e are public keys

p, q are private keys for finding d for any e

(with the condition that $\gcd(e, (p-1)(q-1)) = 1$)

Key Idea:

Everyone knows n (= pq) and e, but to find d to decrypt, need to know what p and q are.

Practically impossible to factor n into p and q if p and q are chosen to be primes of 200 digits or more.

Encryption example: $p = 43 \quad q = 59 \quad e = 13$

$$n = p \cdot q = 2537$$

$$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$$

Message to encrypt: "STOP"

Translate to equivalent numbers

"18 19 14 15"

Group into blocks of two numbers

"1819 1415"

Apply encryption function
to each block

"1819 1415"

$$f(x) = x^e \bmod n$$

$$= x^{13} \bmod 2537$$

Encrypted message: "2081 2182"

Use fast modular exponentiation algorithm:

$$f(1819) = 1819^{13} \bmod 2537 = 2081$$

$$f(1415) = 1415^{13} \bmod 2537 = 2182$$

Message decryption

M :an original block of the message

"1819 1415"

$\downarrow$ encrypt

"2081 2182"

C :respective encrypted block

$$C \equiv M^e \pmod{n}$$

We want to recover M by knowing C, p, q, e

Let d = inverse of e modulo $(p-1)(q-1)$

$$de \equiv 1(\mathrm{mod}(p-1)(q-1))$$

by definition of congruent

$$de = 1 + k(p-1)(q-1)$$

Does inverse d always exist?

Inverse exists because $\gcd(e,(p-1)(q-1)) = 1$

$$\gcd(e,(p-1)(q-1)) = 1 = se + t(p-1)(q-1)$$

i.e., $1 \equiv se \bmod (p-1)(q-1)$

$$\Downarrow$$

$$d = s$$

Encryption $C \equiv M^e \pmod{n}$

Decryption $C^d \equiv \left(M^e\right)^d \pmod{n}$

$$de = 1 + k(p-1)(q-1)$$

$$C^d \equiv M^{de} \equiv M^{1+k(p-1)(q-1)} \pmod{n}$$

In real-world case, $\gcd(M, p) = 1$

(because p is a large prime and M is small)

Remember me?

$$\gcd(M, p) = 1$$

By Fermat's little theorem

$$M^{p-1} \equiv 1 \pmod{p}$$

$$M^{p-1} \equiv 1 \pmod{p}$$

$$\downarrow$$

$$\left(M^{p-1}\right)^{k(q-1)} \equiv 1^{k(q-1)} \equiv 1 \pmod{p}$$

$$\downarrow$$

$M \equiv M \pmod{p}$

Multiply under mod

$$M \cdot \left(M^{p-1}\right)^{k(q-1)} \equiv M \cdot 1 \pmod{p}$$

$$\downarrow$$

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{p}$$

We showed:

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{p}$$

By symmetry (by replacing p with q):

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{q}$$

By Exercise 23 (Sec. 3.7):

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{pq} \equiv M \pmod{n}$$

We showed:

$$\left.\begin{aligned} C^d &\equiv M^{1+k(p-1)(q-1)} \pmod{n} \\ M^{1+k(p-1)(q-1)} &\equiv M \pmod{n} \end{aligned}\right\} \Rightarrow C^d \equiv M \pmod{n}$$

In other words, the original message:

$$M = C^d \bmod n$$

Decryption example: $p = 43 \quad q = 59 \quad e = 13$

$$n = p \cdot q = 2537$$

$$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$$

Compute d = inverse of e modulo $42 \cdot 58$ = 937

"2081 2182"

$$M = C^d \bmod n$$

$$2081^{937} \bmod 2537 = 1819 \qquad 2182^{937} \bmod 2537 = 1415$$

"1819 1415"

"18 19 14 15" = "STOP"